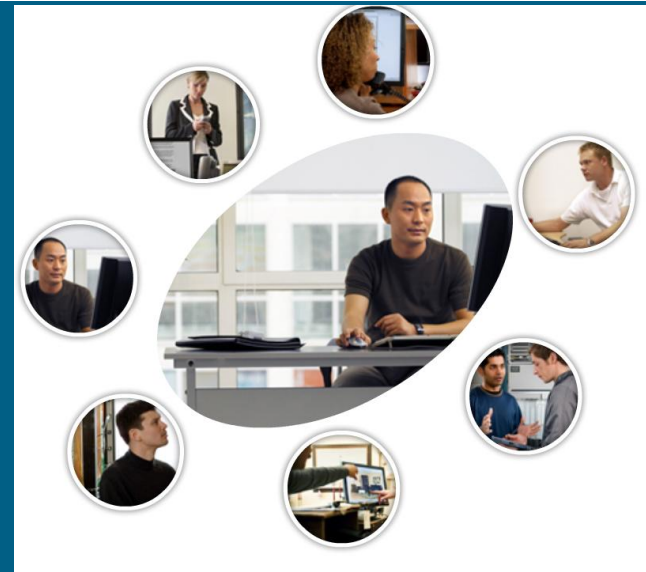




Implementing IP Addressing Services



Accessing the WAN – Chapter 7

Objectives

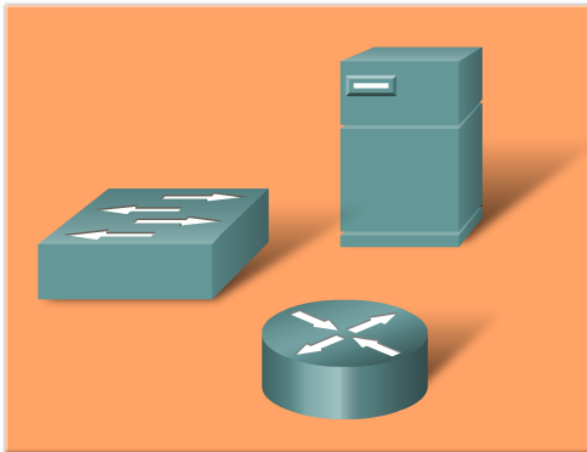
- Configure DHCP in an enterprise branch network
- Configure NAT on a Cisco router
- Configure new generation RIP (RIPng) to use IPv6

Configure DHCP in an Enterprise Branch Network

- Describe the function of DHCP in a network

Introducing DHCP

Manual Configuration



Network devices that remain in the same place (logically and physically) are assigned static IP addresses.

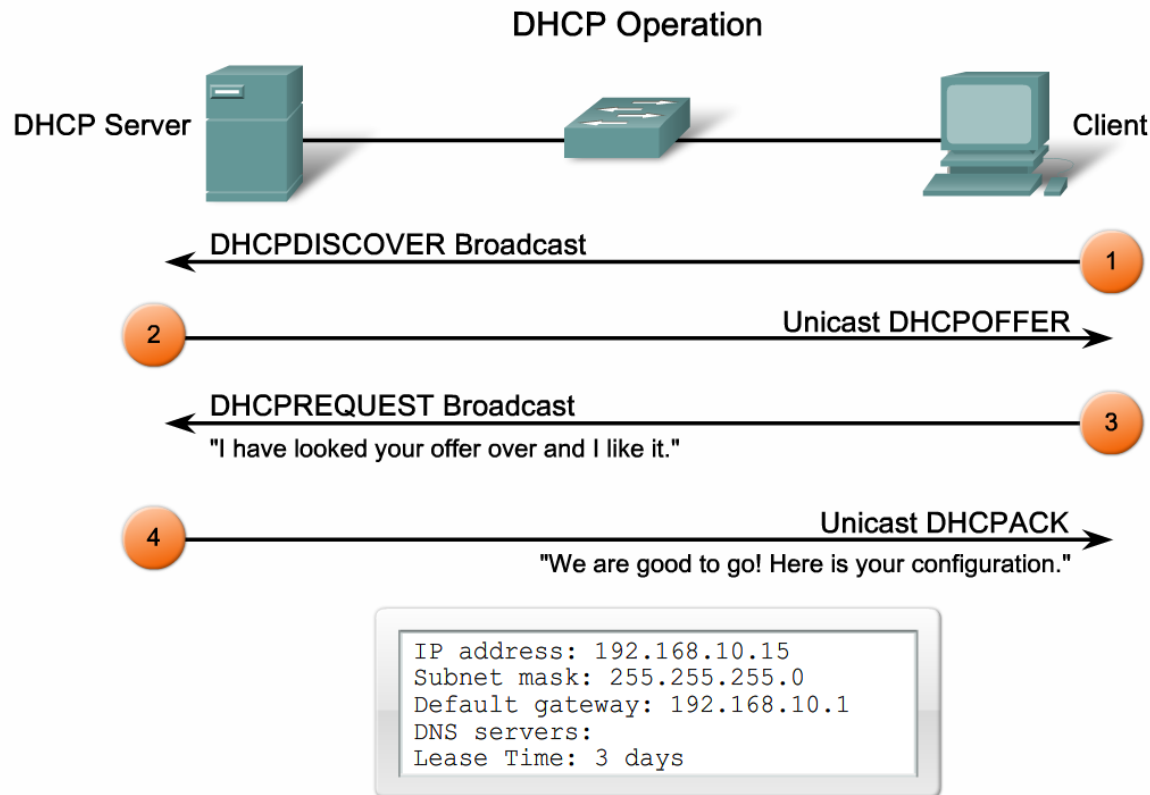
Dynamic Configuration



Network devices that are added, moved or changed (physical and logical) need new addresses. Manual configuration is unwieldy.

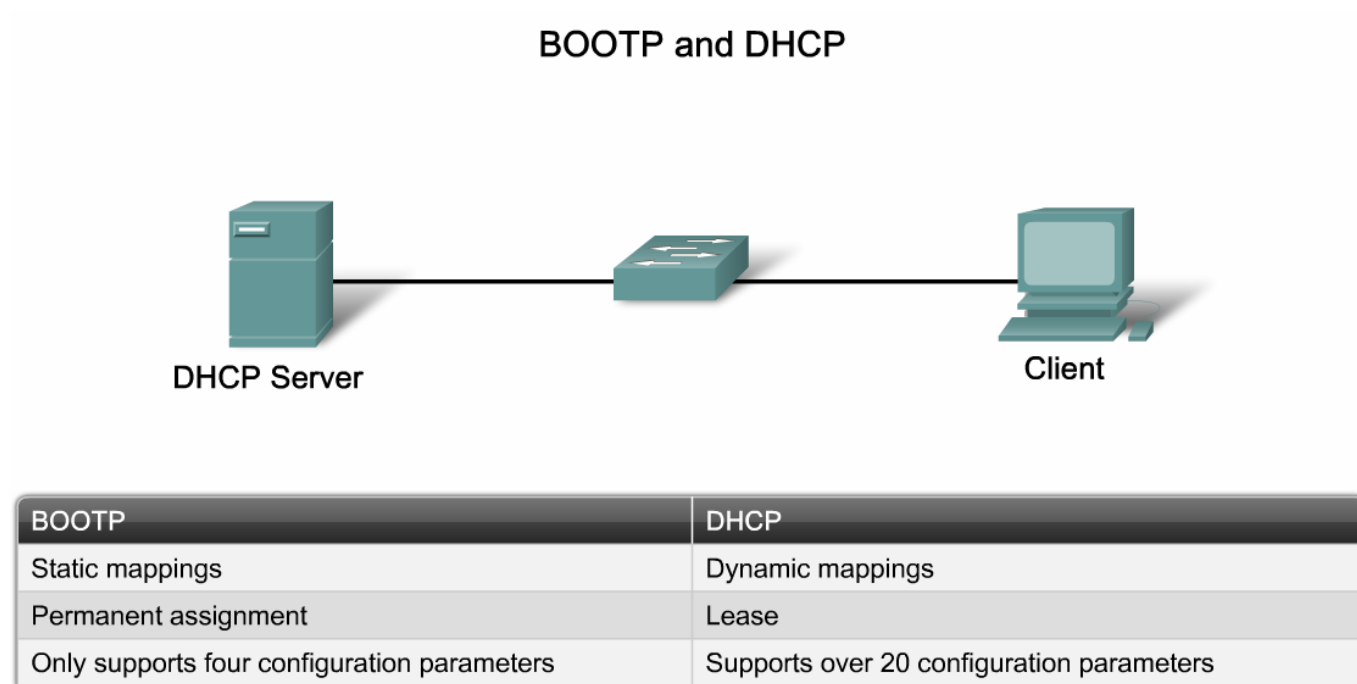
Configure DHCP in an Enterprise Branch Network

- Describe how DHCP dynamically assigns an IP address to a client



Configure DHCP in an Enterprise Branch Network

- Describe the differences between BOOTP and DHCP



Configure DHCP in an Enterprise Branch Network

- Describe how to configure a DHCP server

Configuring DHCP Step 1: Excluding IP Addresses

```
R1 (config)#ip dhcp excluded-address low-address [high-address]
```

```
R1 (config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9  
R1 (config)#ip dhcp excluded-address 192.168.10.254
```

Configure DHCP in an Enterprise Branch Network

- Describe how to configure a Cisco router as a DHCP client

Linksys WAN Connection

The screenshot displays the Linksys WAN Connection configuration interface. The top header includes the Linksys logo, "A Division of Cisco Systems, Inc.", and the firmware version "1.0.00.00". The main navigation bar shows "Setup" as the active tab, with other options like Wireless, Firewall, VPN, QoS, Administration, IPS, L2 Switch, and Status. Below this, a sub-navigation bar lists "IP Versions", "WAN" (selected), "LAN", "DMZ", "MAC Address Clone", "Advanced Routing", and "Time". The "WAN" section is expanded, showing "Optional Settings". The "Internet Connection Type" is set to "Automatic Configuration - DHCP". Below this, there are input fields for "Host Name", "Domain Name", "MTU" (set to "Auto"), and "Size" (set to "1500"). The "DDNS Service" is set to "Disabled". A "More..." link is present on the right side of the page. At the bottom, there are "Save Settings" and "Cancel Changes" buttons. The Cisco Systems logo is visible in the bottom right corner.

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 1.0.00.00

Wireless N Gigabit Security Router with VPN WRT54GL

Setup Wireless Firewall VPN QoS Administration IPS L2 Switch Status

IP Versions | WAN | LAN | DMZ | MAC Address Clone | Advanced Routing | Time

WAN

Optional Settings

Internet Connection Type: Automatic Configuration - DHCP

Host Name:

Domain Name:

MTU: Auto

Size: 1500

DDNS Service: Disabled

The WAN screen you will see when accessing the Router. Most users will be able to configure the Router and get it working properly using only the settings on this screen. Some Internet Service Providers (ISPs) will require that you enter specific information, such as User Name, Password, Internet IP Address, Default Gateway Address, or DNS Address. This information can be obtained from your ISP, if required.

More...

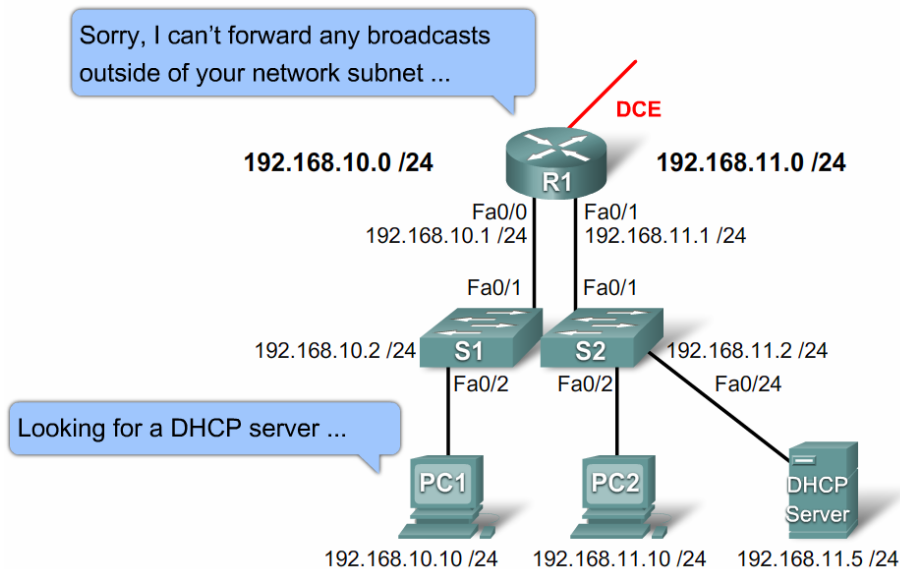
Save Settings Cancel Changes

CISCO SYSTEMS

Configure DHCP in an Enterprise Branch Network

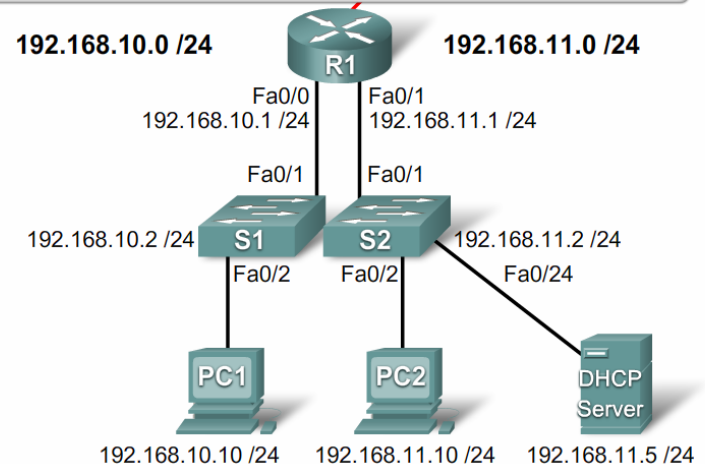
- Explain how DHCP Relay can be used to configure a router to relay DHCP messages when the server and the client are not on the same segment

DHCP Problems



DHCP Relay

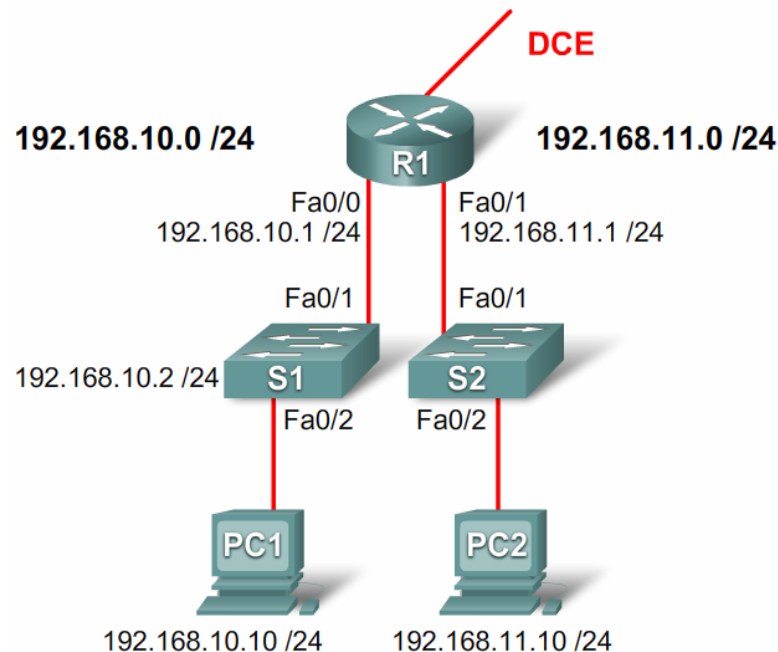
```
R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
```



Configure DHCP in an Enterprise Branch Network

- Describe how to configure a Cisco router as a DHCP client using SDM

Configuring a DHCP Client using SDM



Configure DHCP in an Enterprise Branch Network

- Describe how to troubleshoot a DHCP configuration

Troubleshooting DHCP Configurations

Troubleshooting DHCP	
Troubleshooting Task 1:	Resolving IP Address Conflicts
Troubleshooting Task 2:	Verify Physical Connectivity
Troubleshooting Task 3:	Test Network Connectivity by Configuring Client Workstation with a Static IP Address
Troubleshooting Task 4:	Verify Switch Port Configuration (STP Portfast and Other Commands)
Troubleshooting Task 5:	Distinguishing whether DHCP Clients Obtain IP Address on the Same Subnet or VLAN as DHCP Server

Configure NAT on a Cisco Router

- Describe the operation and benefits of using private and public IP addressing

Public and Private Internet Addresses



Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

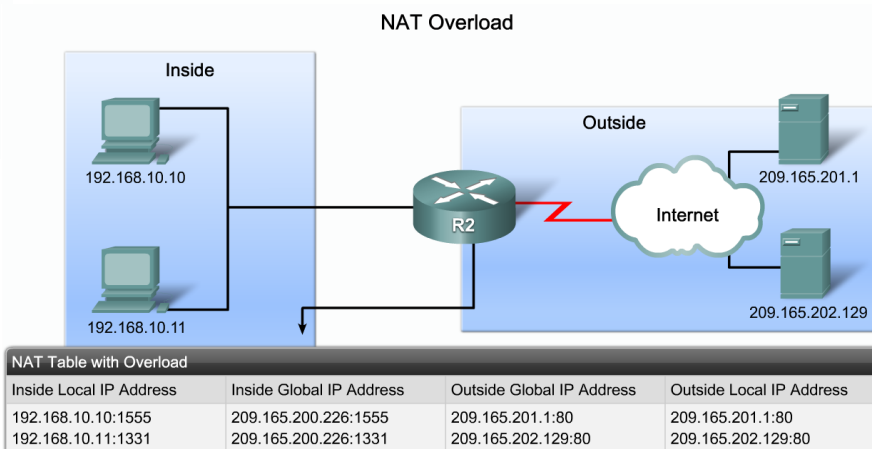
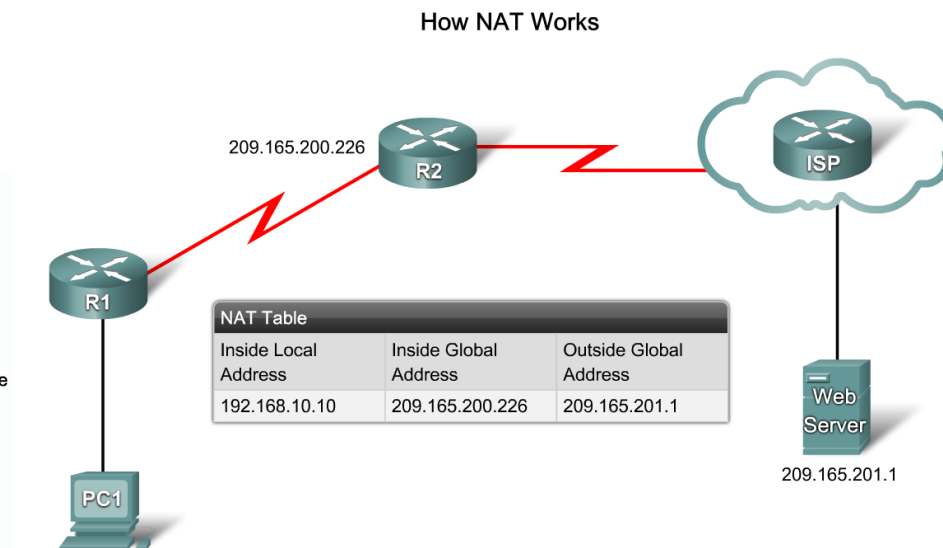
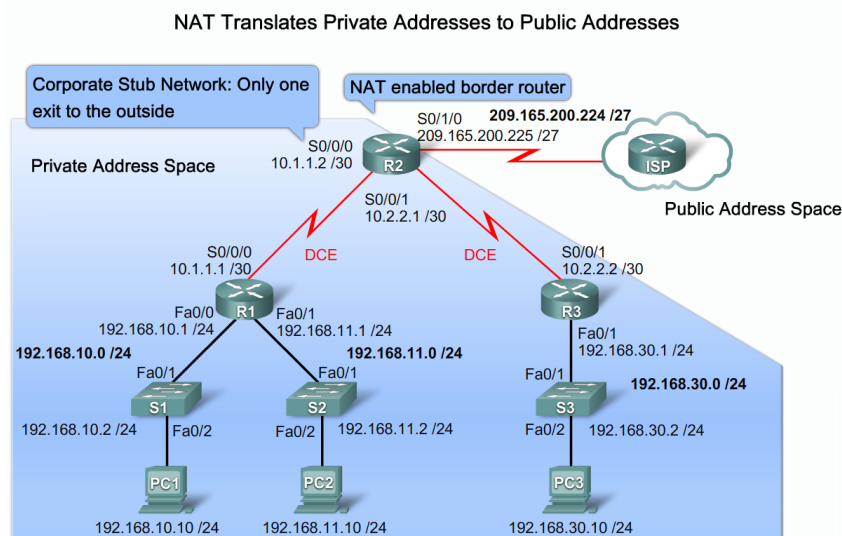
- ARIN
- RIPE
- APNIC
- LACNIC
- AfricNIC

Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Configure NAT on a Cisco Router

- Explain the key features of NAT and NAT overload



Configure NAT on a Cisco Router

- Explain the advantages and disadvantages of NAT

NAT Benefits and Drawbacks

NAT Benefits

- Conserves the legally registered addressing scheme
- Increases the flexibility of connections to the public network
- Provides consistency for internal network addressing schemes.
- Provides network security

NAT Drawbacks

- Performance is degraded
- End-to-end functionality is degraded
- End-to-end IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connections can be disrupted
- Architectures need to be rebuilt to accommodate changes

Configure NAT on a Cisco Router

- Describe how to configure static NAT to conserve IP address space in a network

Configuring Static NAT

Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. Router(config)# ip nat inside source static <i>local-ip global-ip</i>	Enter the global command no ip nat inside source static to remove the static source translation.
2	Specify the inside interface. Router(config)# interface <i>type number</i>	Enter the interface command. The CLI prompt will change from (config) # to (config-if) #.
3	Mark the interface as connected to the inside. Router(config-if)# ip nat inside	
4	Exit interface configuration mode. Router(config-if)# exit	
5	Specify the outside interface. Router(config)# interface <i>type number</i>	
6	Mark the interface as connected to the outside. Router(config-if)# ip nat outside	

Configure NAT on a Cisco Router

- Describe how to configure dynamic NAT to conserve IP address space in a network

Configuring Dynamic NAT

Step	Action	Notes
1	Define a pool of global addresses to be allocated as needed. Router(config)# ip nat pool name start-ip end-ip { netmask netmask prefix-length prefix-length }	Enter the global command no ip nat pool name to remove the pool of global addresses.
2	Define a standard access list permitting those addresses that are to be translated. Router(config)# access-list access-list-number permit source [source-wildcard]	Enter the global command no access-list access-list-number to remove the access list.
3	Establish dynamic source translation, specifying the access list defined in the prior step. Router(config)# ip nat inside source list access-list-number pool name	Enter the global command no ip nat inside source to remove the dynamic source translation.
4	Specify the inside interface. Router(config)# interface type number	Enter the interface command. The CLI prompt will change from (config)# to (config-if)#.
5	Mark the interface as connected to the inside. Router(config-if)# ip nat inside	
6	Specify the outside interface. Router(config)# interface type number	
7	Mark the interface as connected to the outside. Router(config-if)# ip nat outside	
8	Exit interface configuration mode. Router(config-if)# exit	

Configure NAT on a Cisco Router

- Describe how to configure NAT Overload to conserve IP address space in a network

NAT Overload Configuration Example

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. Router(config)# access-list <i>acl-number</i> permit <i>source</i> [<i>source-wildcard</i>]	Enter the global command no access-list <i>access-list-number</i> to remove the access list.
2	Establish dynamic source translation, specifying the access list defined in the prior step. Router(config)# ip nat inside source list <i>acl-number</i> interface <i>interface</i> overload	Enter the global command no ip nat inside source to remove the dynamic source translation. The overload keyword enables PAT.
3	Specify the inside interface. Router(config)# interface <i>type number</i> Router(config-if)# ip nat inside	Enter the interface command. The CLI prompt will change from (config)# to (config-if)#.
4	Specify the outside interface. Router(config-if)# interface <i>type number</i> Router(config-if)# ip nat outside	

NAT Overload Configuration Using a Pool of Public Addresses

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. Router(config)# access-list <i>acl-number</i> permit <i>source</i> [<i>source-wildcard</i>]	Enter the global command no access-list <i>access-list-number</i> to remove the access list.
2	Specify the global address, as a pool, to be used for overloading. Router(config)# ip nat pool <i>name</i> <i>start-ip</i> <i>end-ip</i> { netmask <i>netmask</i> prefix-length <i>prefix-length</i> }.	
3	Establish overload translation. Router { config} # ip nat inside source list <i>acl-number</i> pool <i>name</i> overload .	
4	Specify the inside interface. Router(config)# interface <i>type number</i> Router(config-if)# ip nat inside	Enter the interface command. The CLI prompt will change from (config)# to (config-if)#.
5	Specify the outside interface. Router(config-if)# interface <i>type number</i> Router(config-if)# ip nat outside	

Configure NAT on a Cisco Router

- Describe how to configure port forwarding

Port Forwarding

LINKSYS
A Division of Cisco Systems, Inc.

FW Version: V1.00.12

Wireless-N Gigabit Security Router with VPN WRVS4400H

Firewall

Setup Wireless Firewall VPN QoS Administration IPS L2 Switch Status

Basic Settings IP Based ACL Internet Access Policy Single Port Forwarding Port Range Forwarding More ... >>

Single Port Forwarding

Application	External Port	Internal Port	Protocol	IP Address	Enabled
HTTP	80	80	TCP	192.168.1.0	<input type="checkbox"/>
FTP	21	21	TCP	192.168.1.0	<input type="checkbox"/>
FTP-Data	20	20	TCP	192.168.1.0	<input type="checkbox"/>
Telnet	23	23	TCP	192.168.1.0	<input type="checkbox"/>
SMTP	25	25	TCP	192.168.1.0	<input type="checkbox"/>
TFTP	69	69	UDP	192.168.1.0	<input type="checkbox"/>
finger	79	79	TCP	192.168.1.0	<input type="checkbox"/>
NTP	123	123	UDP	192.168.1.0	<input type="checkbox"/>
POP3	110	110	TCP	192.168.1.0	<input type="checkbox"/>

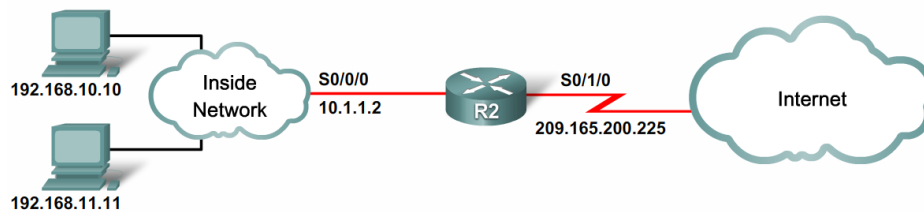
Use the Single Port Forwarding screen when you want to open specific services (that use single port). This allows users on the Internet to access this server by using the WAN port address and the matched external port number. When users send these types of request to your WAN port IP address via the Internet, the NAT Router will forward those requests to the appropriate servers on your LAN.

[More...](#)

Configure NAT on a Cisco Router

- Describe how to verify and troubleshoot NAT and NAT overload configurations

NAT Overload Configuration Example



```
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface serial 0/0/0
 ip nat inside
interface serial 0/1/0
 ip nat outside
```

Debug NAT Translations

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Oct 6 19:55:31.579: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14434]
*Oct 6 19:55:31.595: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6334]
*Oct 6 19:55:31.611: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14435]
*Oct 6 19:55:31.619: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14436]
*Oct 6 19:55:31.627: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14437]
*Oct 6 19:55:31.631: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6335]
*Oct 6 19:55:31.643: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6336]
*Oct 6 19:55:31.647: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14438]
*Oct 6 19:55:31.651: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6337]
*Oct 6 19:55:31.655: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14439]
*Oct 6 19:55:31.659: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6338]

<Output omitted>
```

Configure New Generation RIP (RIPng) to use IPv6

- Explain the need for IPv6 to provide a long-term solution to the depletion problem of IP address

Assigned IP Address Blocks

Blocks Assigned - 1993

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

- Allocated
- Unavailable
- Available

Configure New Generation RIP (RIPng) to use IPv6

- Describe the format of the IPv6 addresses and the appropriate methods for abbreviating them

IPv6 Address Representation

IPv6 Formats

Format:

- **x:x:x:x:x:x:x:x**, where x is a 16-bit hexadecimal field
 - Case-insensitive for hexadecimal A, B, C, D, E, and F
- Leading zeros in a field are optional
- Successive fields of zeros can be represented as **::** only once per address

Examples:

- **2031:0000:130F:0000:0000:09C0:876A:130B**
 - Can be represented as **2031:0:130f::9c0:876a:130b**
 - Cannot be represented as **2031::130f::9c0:876a:130b**
- **FF01:0:0:0:0:0:0:1** **FF01::1**
- **0:0:0:0:0:0:0:1** **::1**
- **0:0:0:0:0:0:0:0** **::**

Configure New Generation RIP (RIPng) to use IPv6

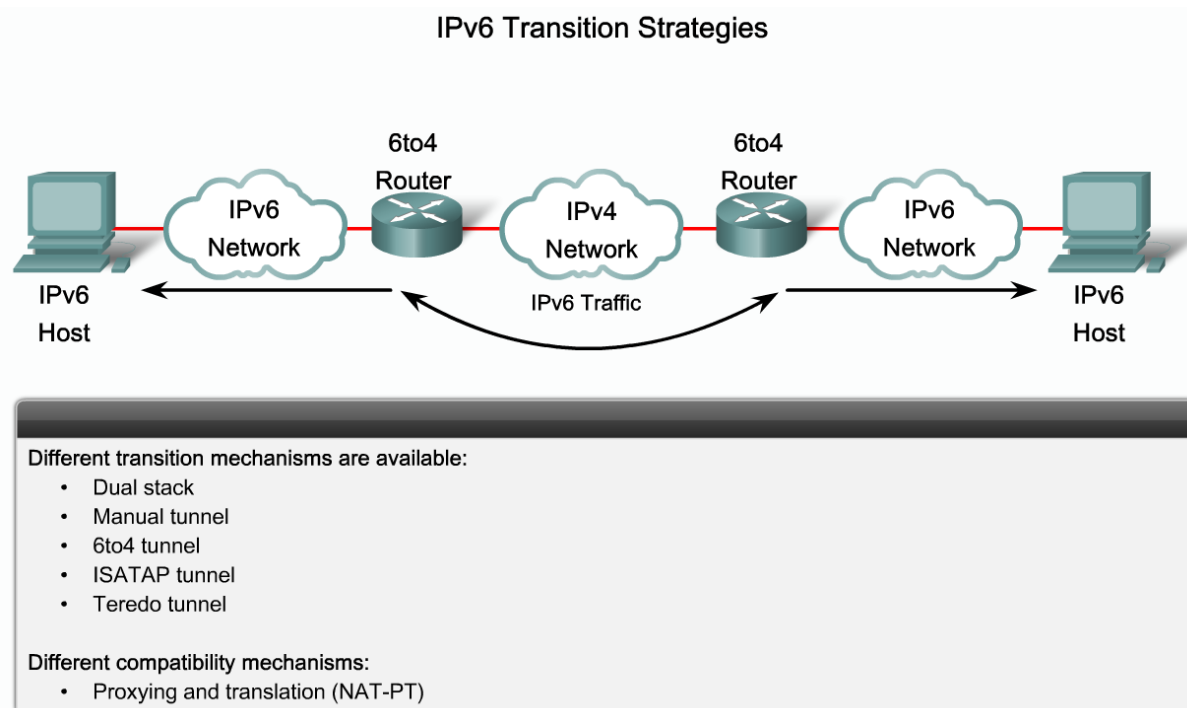
- Explain the various methods of assigning IPv6 addresses to a device

Assigning IPv6 Addresses

Static assignment	Dynamic assignment
<ul style="list-style-type: none">• Manual interface ID assignment• EUI-64 interface ID assignment	<ul style="list-style-type: none">• Stateless autoconfiguration• DHCPv6 (stateful)

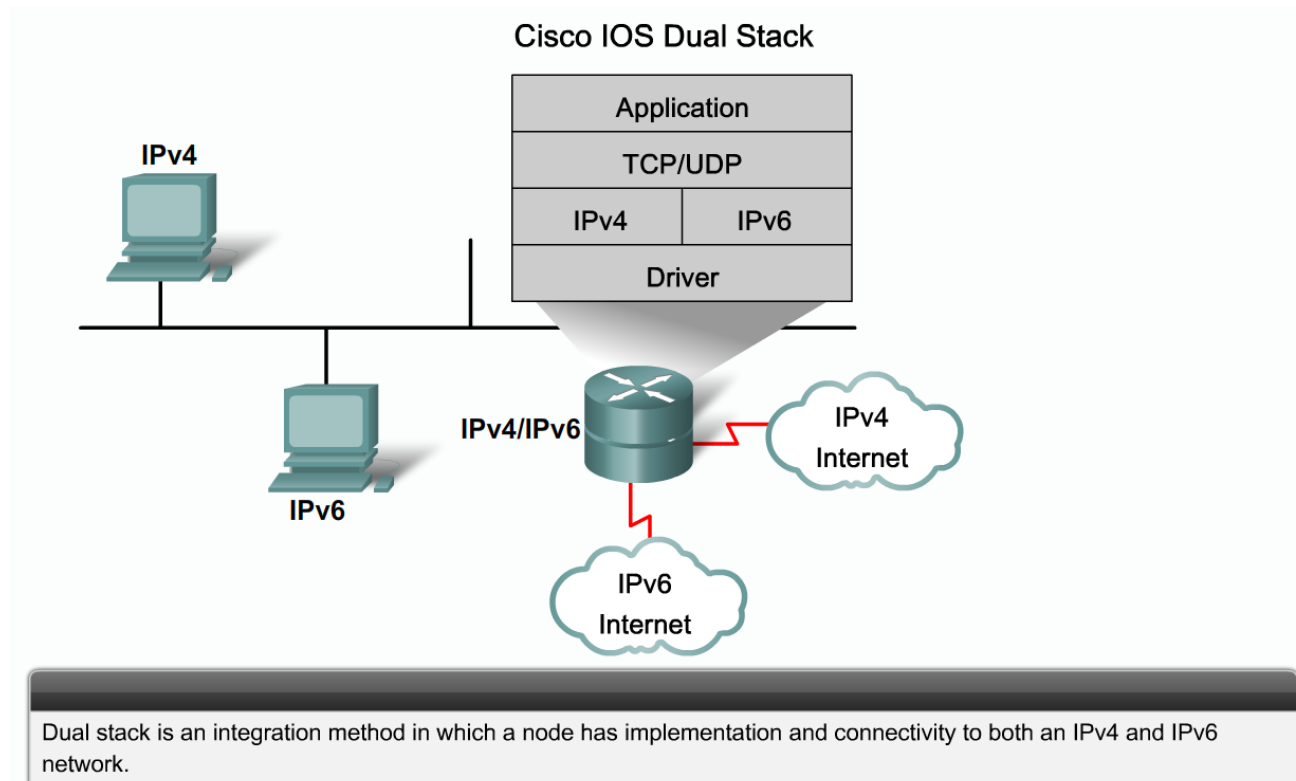
Configure New Generation RIP (RIPng) to use IPv6

- Describe the transition strategies for implementing IPv6



Configure New Generation RIP (RIPng) to use IPv6

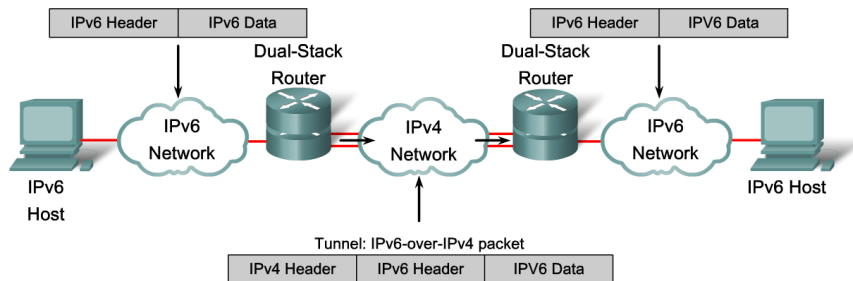
- Describe how Cisco IOS dual stack enables IPv6 to run concurrently with IPv4 in a network



Configure New Generation RIP (RIPng) to use IPv6

- Describe the concept of IPv6 tunneling

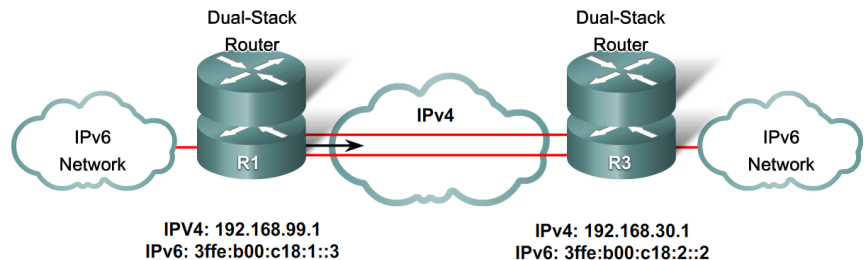
IPv6 Tunneling



Tunneling is an integration method in which an IPv6 packet is encapsulated within another protocol, such as IPv4. This method of encapsulation is IPv4:

- Includes a 20-byte IPv4 header with no options and an IPv6 header and payload
- Requires dual-stack routers

Manually Configured IPv6 Tunnel



Configured tunnels require:

- Dual-stack endpoints
- IPv4 and IPv6 addresses configured at each end

Configure New Generation RIP (RIPng) to use IPv6

- Describe how IPv6 affects common routing protocols, and how these protocols are modified to support IPv6

RIPng Routing Protocol

Similar IPv4 features:

- Distance vector, radius of 15 hops, split horizon, and poison reverse
- Based on RIPv2

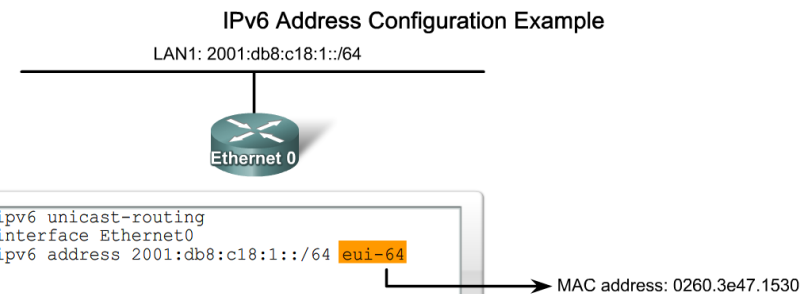
Updated features for IPv6:

- IPv6 prefix, next-hop IPv6 address
- Uses the multicast group FF02::9, the all-rip-routers multicast group, as the destination address for RIP updates
- Uses IPv6 for transport
- Named RIPng

Configure New Generation RIP (RIPng) to use IPv6

- Explain how to configure a router to use IPv6

Enabling IPv6 on Cisco Routers



```
RouterX# show ipv6 interface Ethernet0
Ethernet0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
Global unicast address(es):
2001:DBB:C18:1::260:3EFF:FE47:1530, subnet is 2001:DBB:C18:1::/64
Joined group address(es):
FF02::1:FE47:1530
FF02::1
FF02::2
MTU is 1500 bytes
```

Command	Purpose
RouterX(config) # ipv6 unicast-routing	Enables IPv6 traffic forwarding
RouterX(config-if) # ipv6 address ipv6prefix/prefix-length eui-64	Configures the interface IPv6 addresses

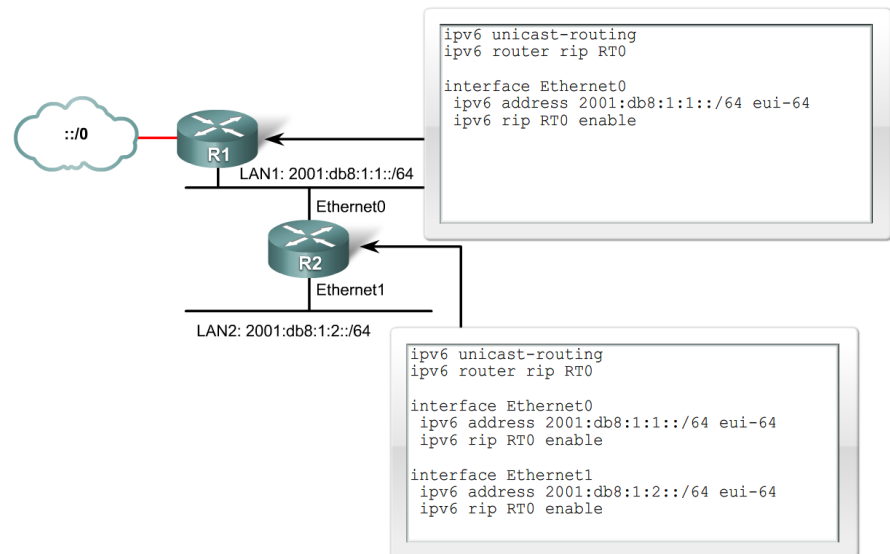
Configure New Generation RIP (RIPng) to use IPv6

- Explain how to configure and verify RIPng for IPv6

Configuring RIPng for IPv6

Command	Purpose
RouterX(config)# ipv6 router rip name	Creates and enters RIP router configuration mode.
RouterX(config-if)# ipv6 rip name enable	Configures RIP on an interface.

RIPng for IPv6 Configuration



Configure New Generation RIP (RIPng) to use IPv6

- Explain how to verify and troubleshoot IPv6

Commands	
Command	Purpose
<code>show ipv6 interface</code>	Displays the status of interfaces configured for IPv6.
<code>show ipv6 interface brief</code>	Displays a summarized status of interfaces configured for IPv6.
<code>show ipv6 neighbors</code>	Displays IPv6 neighbor discovery cache information.
<code>show ipv6 protocols</code>	Displays the parameters and current state of the active IPv6 routing protocol processes.
<code>show ipv6 rip</code>	Displays information about the current
<code>show ipv6 route</code>	Displays the current IPv6 routing table.
<code>show ipv6 route summary</code>	Displays a summarized form of the current IPv6 routing table.
<code>show ipv6 routers</code>	Displays IPv6 router advertisement information received from other routers.
<code>show ipv6 static</code>	Displays only static IPv6 routes installed in the routing table.
<code>show ipv6 static 2001:db8:5555:0/16</code>	Displays only static route information about the specific address given.
<code>show ipv6 static interface serial 0/0</code>	Displays only static route information with the specified interface as the outgoing interface.
<code>show ipv6 static detail</code>	Displays a more detailed entry for IPv6 static routes.
<code>show ipv6 traffic</code>	Displays statistics about IPv6 traffic.

Summary

- Dynamic Host Control Protocol (DHCP)

This is a means of assigning IP address and other configuration information automatically.

- DHCP operation

- 3 different allocation methods

- Manual
 - Automatic
 - Dynamic

- Steps to configure DHCP

- Define range of addresses
 - Create DHCP pool
 - Configure DHCP pool specifics

Summary

- DHCP Relay

Concept of using a router configured to listen for DHCP messages from DHCP clients and then forwards those messages to servers on different subnets

- Troubleshooting DHCP

- Most problems arise due to configuration errors
- Commands to aid troubleshooting
 - Show ip dhcp
 - Show run
 - debug

Summary

- Private IP addresses
 - Class A = 10.x.x.x
 - Class B = 172.16.x.x – 172.31.x.x
 - Class C = 192.168.x.x
- Network Address Translation (NAT)
 - A means of translating private IP addresses to public IP addresses
 - Types of NAT
 - Static
 - Dynamic
 - Some commands used for troubleshooting
 - Show ip nat translations
 - Show ip nat statistics
 - Debug ip nat

Summary

- IPv6
 - A 128 bit address that uses colons to separate entries
 - Normally written as 8 groups of 4 hexadecimal digits
- Cisco IOS Dual Stack
 - A way of permitting a node to have connectivity to an IPv4 & IP v6 network simultaneously
- IPv6 Tunneling
 - An IPV6 packet is encapsulated within another protocol

Summary

- Configuring RIPng with IPv6

- 1st globally enable IPv6

- 2nd enable IPv6 on interfaces on which IPv6 is to be enabled

- 3rd enable RIPng using either

- ipv6 router *name*

- ipv6 router *name* enable

